



SECS 1030

labo Phishing email

**Noté sur 13 points – 10% de la note finale à rendre pour
jeudi 17 octobre 2024 dans le casier de dépôt**

Objectif du laboratoire : analyser 3 sources de courriels pour détecter une attaque de Phishing

Outil : un éditeur de fichier txt (notepad, notepad++, ...) ou un éditeur de mail header. Les courriels sont sur Ardoise, Labos, labos email phishing

Exercice 0 : email-0.eml (3 points)

1. Quelle est la valeur dans le champ « from : » ? (text+adresse email)

```
C:\Users\maple\OneDrive - MONCCNB\École\Automne 2024\SECS1030\Laboratoire\Email\email-0.eml - Notepad++
Fichier Édition Recherche Affichage Encodage Langage Paramètres Outils Macro Exécution Modules d'extension Documents ?
email-0.eml email-1 (2).eml
1 Received: from YT1PR01MB8780.CANPRD01.PROD.OUTLOOK.COM (2603:10b6:b01:cb::8)
2 by YQXPR01MB5154.CANPRD01.PROD.OUTLOOK.COM with HTTPS; Mon, 8 May 2023
3 15:56:09 +0000
4 Received: from YT4PR01CA0427.CANPRD01.PROD.OUTLOOK.COM (2603:10b6:b01:10b::18)
5 by YT1PR01MB8780.CANPRD01.PROD.OUTLOOK.COM (2603:10b6:b01:cb::8) with
6 Microsoft SMTP Server (version=TLS1_2,
7 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6363.32; Mon, 8 May
8 2023 15:56:06 +0000
9 Received: from YT3CAN01FT006.eop-CAN01.prod.protection.outlook.com
10 (2603:10b6:b01:10b:cafe::a) by YT4PR01CA0427.outlook.office365.com
11 (2603:10b6:b01:10b::18) with Microsoft SMTP Server (version=TLS1_2,
12 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6363.32 via Frontend
13 Transport; Mon, 8 May 2023 15:56:06 +0000
14 Authentication-Results: spf=none (sender IP is 153.125.140.170)
15 smtp.mailfrom=riv-round.com; dkim=none (message not signed)
16 header.d=none; dmarc=none action=none header.from=riv-round.com; compauth=fail
17 reason=001
18 Received-SPF: None (protection.outlook.com: riv-round.com does not designate
19 permitted sender hosts)
20 Received: from www4330.sakura.ne.jp (153.125.140.170) by
21 YT3CAN01FT006.mail.protection.outlook.com (10.118.140.178) with Microsoft
22 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
23 15.20.6387.18 via Frontend Transport; Mon, 8 May 2023 15:56:05 +0000
24 Received: from fsav314.sakura.ne.jp (fsav314.sakura.ne.jp [153.120.85.145])
25 by www4330.sakura.ne.jp (8.15.2/8.15.2) with ESMTP id 348Fu3vW057836
26 for <adresse-email@anonymise>; Tue, 9 May 2023 00:56:03 +0900 (JST)
27 (envelope-from info@riv-round.com)
28 Received: from www4330.sakura.ne.jp (153.125.140.170)
29 by fsav314.sakura.ne.jp (F-Secure/fsigk_smtp/550/fsav314.sakura.ne.jp);
30 Tue, 09 May 2023 00:56:03 +0900 (JST)
31 X-Virus-Status: clean(F-Secure/fsigk_smtp/550/fsav314.sakura.ne.jp)
32 Received: from WIN-JIGMJ51T9LR (ec2-35-78-188-208.ap-northeast-1.compute.amazonaws.com [35.78.188.208])
33 (authenticated bits=0)
34 by www4330.sakura.ne.jp (8.15.2/8.15.2) with ESMTPA id 348Fu36x057831
35 for <adresse-email@anonymise>; Tue, 9 May 2023 00:56:03 +0900 (JST)
36 (envelope-from info@riv-round.com)
37 Message-Id: <202305081556.348Fu36x057831@www4330.sakura.ne.jp>
38 From: =?utf-8?Q?=28CRA=29=C2=AE_Canadian=2DRevenue_Agency?=
39 <info@riv-round.com>
40 To: adresse-email@anonymise
41 Date: 8 May 2023 15:56:03 +0000
42 Subject: =?utf-8?B?wq5SYXBwZWwgZGUgbOKAmUFnZW5jZSBkdSB5ZyZlbnUgZHUg?=
```

2. Dans le champ « from : », le texte (partie gauche) est-il cohérent avec l'adresse (partie entre <>) ?
Non il n'est pas cohérent
3. Faites une recherche whois sur le domaine de l'adresse de « from : ». Quel est le nom et pays du registrant ? Pouvez-vous en déduire si ce courriel est un spoofing email ? Si oui pourquoi ?

SHOTA OMARU, Japon, Je dirais que oui puisque le email est envoyer avec riv-round.com mais le message dit que ça vient de l'agence de revenu du Canada. C'est très suspect.

Exercice 1 : email1.eml (6 points)

1. Quel est le champ « from : » ? (text+adress)
?UTF-8?B?Y2hyb25vLXBvc3RILWV4cHJlc3M=?" <GNxHHUed@gktlbnC.us>
Dans le champ « from : » , le texte est-il cohérent avec l'adresse ?

Non
2. Est-ce que l'adresse email du champ « return_path » est la même que le champs « from: » ?

non
3. Quel est le résultat de SPF ? Qu'est ce que ce résultat signifie ?
Pass , l'adresse de retour est autorisé à envoyé
4. L'email contient-il un ou des liens ? Sur quel site pourriez-vous vérifiez ce lien ?

Oui, virus total, url extractor, phishtool
5. Selon vous ce mail est-il un spam email ou un phishing email ?

phishing

Exercice 2 : Questions (4 points)

1. Quelle commande permet d'afficher les adresses IP des serveurs emails autorisés pour le domaine outlook.com ? Montrez une capture écran du résultat :

Dig TXT outlook.com +short
2. SPF : pour le domaine outlook.com, que signifie le mechasnism « ~all » à la fin de la ressource TXT « spf » du DNS record ?

Il accpete les messages provenant d'expediteur qui ne figure pas dans l'enregistrement SPF, il les marque comme suspect.
3. Quelle commande permet d'afficher la clé publique du domaine gmail.com avec le selector 20230601 ?

dig TXT 20230601._domainkey.gmail.com

4. Quelle commande permet d'afficher la règle DMARC pour le domaine outlook.com ?

Dig TXT _dmarc.outlook.com